



FortiAuthenticator - Release Notes

Version 6.0.3

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 19, 2021

FortiAuthenticator 6.0.3 Release Notes

23-603-583129-20210819

TABLE OF CONTENTS

Change log	4
FortiAuthenticator 6.0.3 release	5
Special notices	6
TFTP boot firmware upgrade process	6
Monitor settings for GUI access	6
Before any firmware upgrade	6
After any firmware upgrade	6
What's new	7
SAML SP single logout enhancements for FSSO	7
SAML remote authentication enhancements	7
Low HA sync activity SNMP trap	7
Reject usernames containing uppercase letters	7
Upgrade instructions	8
Hardware and VM support	8
Image checksums	8
Upgrading from FortiAuthenticator 4.x/5.x/6.0.x	9
Product integration and support	11
Web browser support	11
FortiOS support	11
Fortinet agent support	11
Virtualization software support	12
Third-party RADIUS authentication	12
FortiAuthenticator-VM	13
FortiAuthenticator-VM system requirements	13
FortiAuthenticator-VM sizing guidelines	13
FortiAuthenticator-VM firmware	14
Resolved issues	15
Known issues	18
Maximum values for hardware appliances	20
Maximum values for VM	22

Change log

Date	Change Description
2019-10-09	Initial release.
2019-11-01	Added additional information about supported VM environments: Product integration and support on page 11
2021-08-19	Updated Product integration and support on page 11 .

FortiAuthenticator 6.0.3 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.0.3, build 0058.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: <https://docs.fortinet.com/product/fortiauthenticator/>

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. Go to **System > Dashboard > Status** and select **Backup/Restore > Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

What's new

FortiAuthenticator version 6.0.3 includes the following new features and enhancements:

SAML SP single logout enhancements for FSSO

New enhancements have been introduced for SAML SP single logout for FSSO:

- Support for the handling of IdP-initiated logout.
- The logout button on the **SAML SP Logout Page** replacement message also triggers a logout from the IdP.
- A new button has been added to the **SAML SP Logout Success Page** replacement message to return to the login page.

SAML remote authentication enhancements

FortiAuthenticator SPs include the "RequestedAuthnContext" assertion in their authentication request to any IdP. FortiAuthenticator 6.0.3 now includes a setting to define the authentication context value.

The **Default** value is "PasswordProtectedTransport," which requires that users are authenticated using a password-based method. When alternative authentication methods are used, **None** can be selected to omit this requirement (e.g. when a X.509 certificate is used in Azure).

Low HA sync activity SNMP trap

A new "HA sync activity is low" trap is available that can be used by administrators to monitor the health of the HA cluster. The SNMP trap is sent by the cluster's standby member. To use this trap, create or edit an SNMPv1/v2c/v3 at **System > Administration > SNMP** and enable the toggle for "HA sync activity is low."

Reject usernames containing uppercase letters

FortiAuthenticator includes the option to reject usernames that contain uppercase letters when using RADIUS authentication. When the option is enabled, RADIUS authentication automatically fails when the username contains an uppercase letter.

Upgrade instructions



Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the [FortiAuthenticator Administration Guide](#).

Hardware and VM support

FortiAuthenticator 6.0.3 supports:

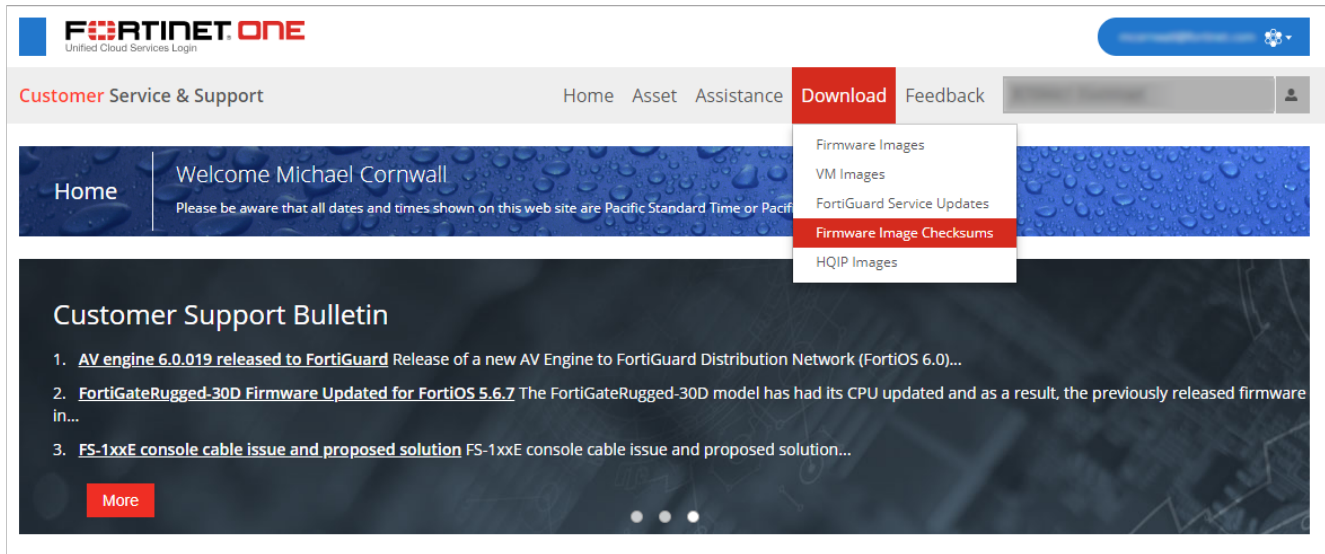
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, AWS, Azure, and OCI)

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the [Fortinet Support](#) website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x/6.0.x

FortiAuthenticator 6.0.3 build 0058 officially supports upgrade from all versions of FortiAuthenticator 4.x, 5.x, and 6.0.x.

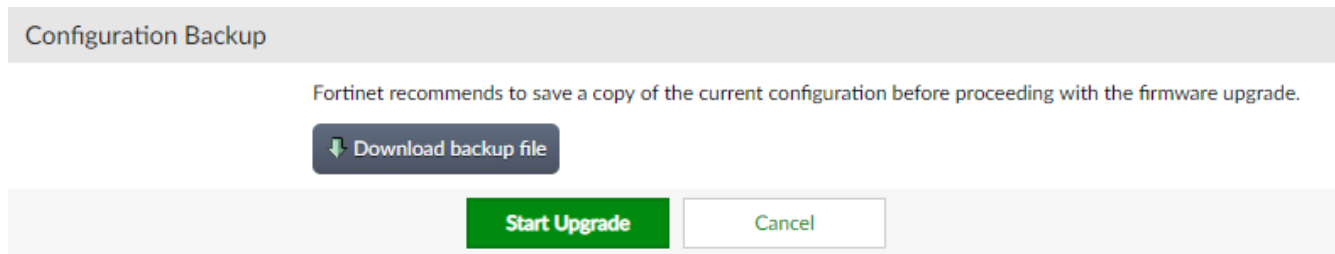
Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the [Fortinet Support](#) website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the [Fortinet Support](#) website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Go to **System > Dashboard > Status**.
5. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
6. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
7. Select **OK** to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.

Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.0.3:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 44
- Mozilla Firefox version 69
- Google Chrome version 77

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.0.3 supports the following FortiOS versions:

- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x
- FortiOS v5.6.x
- FortiOS v5.4.x

Fortinet agent support

FortiAuthenticator 6.0.3 supports the following Fortinet Agents:

- FortiClient v.5.x, v.6.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.3
- FortiAuthenticator Agent for Outlook Web Access 1.6
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Virtualization software support

FortiAuthenticator 6.0.3 supports:

- VMware ESXi / ESX 4/5/6
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, and Hyper-V 2016
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine
- AWS
- Microsoft Azure
- Oracle Cloud Infrastructure



Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See [FortiAuthenticator-VM on page 13](#) for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

FortiAuthenticator-VM

FortiAuthenticator-VM system requirements

The following table provides a detailed summary on FortiAuthenticator virtual machine (VM) system requirements. Installing FortiAuthenticator-VM requires that you have already installed a supported VM environment. For details, see the [FortiAuthenticator VM Install Guide](#).

VM requirements

Virtual machine	Requirement
VM form factor	Open Virtualization Format (OVF)
Virtual CPUs supported (minimum / maximum)	1 / 64
Virtual NICs supported (minimum / maximum)	1 / 4
Storage support (minimum / maximum)	60 GB / 16 TB
Memory support (minimum / maximum)	2 GB / 1 TB
High Availability (HA) support	Yes

FortiAuthenticator-VM sizing guidelines

The following table provides FortiAuthenticator-VM sizing guidelines based on typical usage. Actual requirements may vary based on usage patterns.

VM sizing guidelines

Users	Virtual CPUs	Memory	Storage
1 - 500	1	2 GB	1 TB
500 to 2,500	2	4 GB	1 TB
2,500 to 7,500	2	8 GB	2 TB
7,500 to 25,000	4	16 GB	2 TB
25,000 to 75,000	8	32 GB	4 TB
75,000 to 250,000	16	64 GB	4 TB

Users	Virtual CPUs	Memory	Storage
250,000 to 750,000	32	128 GB	8 TB
750,000 to 2,500,000	64	256 GB	16 TB
2,500,000 to 7,500,000	64	512 GB	16 TB

FortiAuthenticator-VM firmware

Fortinet provides FortiAuthenticator-VM firmware images in two formats:

- **.out**
Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip / kvm.zip / hyperv.zip / xen.zip / opc.zip**
Used for new VM installations.

For more information see the FortiAuthenticator product datasheet available on the [Fortinet web site](#).

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the [Fortinet Support](#) website.

Bug ID	Description
524131	Multisecond delay between queuing and sending of push notifications.
540933	Source IP is missing for authentication requests coming from FortiAuthenticator Windows Agent.
543791	Users Audit report does not update timestamps for LDAP users in "last used" column.
545558	SCEP certificate renewal fails for manually created certificates.
550090	FSSO log show "work queue full, dropping event from ..."
550315	Provide password/SSH key provisioning and recovery in Azure builds.
557762	FortiAuthenticator load balancer unable to synchronize after HA password change.
557771	Active-passive cluster standby member stuck at "standby" if active member down while status is "in_sync."
559457	User can't resize columns in "End Entities" Certificate Management.
561592	Including Remote LDAP Groups to the Self-Registration approval groups causes Django error.
565729	Password reset is not working with RADIUS user on Fortigate having "uppercase" letter.
566765	GUI crashes when registering a new account via guest portal if the account expiry is enabled and account info is displayed on the browser.
567193	SNMP not responding.
569518	When creating an intermediate CA certificate, the certificate is not saved into fs.
569557	In the GUI dashboard, the user inventory widget gets stuck showing only the process running icon.
570317	FortiAuthenticator 6.0.1 is not compatible with FGT 6k/7k.
570602	AD auth failed for remote RADIUS clients with PAP and realm info.
570792	Remote SAML Server's IdP fingerprint matching should be case insensitive.
571219	Remote User Admin can't log-in with backup password.
571244	Guest Portal FortiAuthenticator admin approval link error.
571490	After upgrading from 6.0.0 to 6.0.2 the FortiAuthenticator cannot delete a RADIUS client. It results in "An error has occurred."
571693	Cannot export or delete a CSR created on FortiAuthenticator.
571790	SMBv1 request from FortiAuthenticator to domain controller forti forticlient mobility agent NTLM authentication.

Bug ID	Description
572673	Guest Portal crashes when registering a guest user with admin approval enabled.
573102	Guest Portal User Registration displays error when user requests Click here to resend > Click to continue button.
573440	Firmware Upgrade to 6.0.X overwrites Upgrade History.
573956	Attempting to create and register a new device under guest portal profile results in a crash.
574005	Adding a MAC device HTTP Parameter for Guest Portal results in an error.
574697	Cancel button in "Forms" social login shows 403 error (goes to /guests/ url).
574704	Guest Portal Cancel button doesn't work for self-registration form.
574790	Remote SAML user import from Azure AD fails on authorization issue.
575152	Guest Portal URL links get truncated at the end of new user registration.
575432	Disabling "admin approval required" in self-registration settings doesn't remove the sponsor field in the register form.
575434	Fortitoken Cloud should be disabled if email method is not available.
575894	Non-admin user displayed 500 internal server error when attempting to register a Fortitoken Cloud via token self-registration.
575988	FortiAuthenticator is missing the Proxy-State attribute in its RADIUS Accounting response causing an error on forwarding server.
576459	Unable to sort first name, last name, and email address in User Lookup table.
577123	Error message "Error connecting to database" and GUI login is not available.
577275	Attempting to filter results in RADIUS servers causes a crash error.
577396	FortiAuthenticator dropping RADIUS accounting requests from Microsoft Network Policy Server (NPS).
578192	Missing the "Restore" button under "Backup and restore."
578285	FortiAuthenticator - Apache HTTP Server 2.4.41 released.
579416	The restore default button does not work for the Guest Portal replacement messages.
579651	NTP and Timezone (GMT-6:00) for Central America is the wrong time.
579660	Creating a RADIUS client with a blank name cannot be viewed/deleted/edited in the GUI but takes up an entry.
580493	The online SCEP function is not working on the authenticator.
581226	User Lockout permanently disabling user not working correctly.
581252	Unable to export FortiAuthenticator users database.
581854	CRL export in GUI producing gibberish output.
582157	SAML authentication with Azure AD is not working on latest Microsoft Edge/IE browsers.

Bug ID	Description
583972	New Azure SAML IdP applications rules are incompatible with FAC SAML SP setup.
583294	Detect when joining a domain hangs in the DNS update, and kill <code>net ads join</code> to recover.
584287	The radiusd hangs when waiting for the snmptrap firing to finish, and can recover after <code>diagnose auth restart</code> .
586442	Custom NameID assertion is broken.
555297	On GSuite LDAP, gray out Regular bind type for remote LDAP servers when Secure Connection option is enabled.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please visit the [Fortinet Support](#) website.

Bug ID	Description
445313	Default behavior for FTM de-provision.
478985	FortiAuthenticator Windows Agent sometimes doesn't see the domain name and user is not able to login.
490281	GUI issue with FortiAuthenticator Logging.
510931	Monitor > Authentication > Windows AD statuses.
512913	One of the cluster units doesn't send traps while set as the active member.
519319	FortiAuthenticator is crashing every time when the LDAP Remote user sync rules are supposed to run.
526202	FortiAuthenticator does not check if signature of CSR is valid.
526662	FortiAuthenticator SNMP TRAP on disk failure and/or SNMP OID for disk status.
528231	Log showing "can not add any more users because limit of 1100 has been reached."
528352	FortiAuthenticator HA CLI errors.
529178	FortiAuthenticator 5.5.0 search for serial number in certificate subject.
532652	Users Audit Report not working on load-balancer in cluster.
536211	Should limit FSSO password to 15 characters since that is the limit on the FortiGate.
538059	Importing an ECDSA-signed certificate/key causes an error dump.
540932	FSSOMA nested group search failing if nested via primary group.
541884	FortiAuthenticator drops connection to FortiGate with error "sock_recv() failed, error: 104."
543729	RADIUS client service not working after upgrade.
544691	Remote LDAP admins have no certificate bindings.
544851	Interface in use when HA re-enabled.
546764	Non-ASCII characters in replacement messages cause line-break in the middle of a URL in emails.
551478	FortiAuthenticator-VM upgrade from 4.0 b6237 to 6.0 b010 not successful.
551706	FortiAuthenticator LB HA Cluster cannot have two remote FortiAuthenticator admins with same username when 2FA FortiToken is enabled.
554282	Should have similar log messages for remote sync rule when either admin or non-admin role is assigned to imported user.
555180	Push notification certificates not restored to disk following model conversion.
555320	Captive Portal Time schedule for Device only (MAC address) is not working

Bug ID	Description
561563	Guest Portal authentication fails with HTTP 500 if user's name contains non-ASCII characters.
561588	Adding an SMS license shows "connection timeout" in the GUI.
563330	Error while accessing Authentication > Remote Users .
565635	When FortiAuthenticator receives AVP with multiple VSA for MSCHAP-v2 it rejects the 2nd request (response to challenge).
566145	Usage Profile "TIME USAGE=Time used" is not triggering COA or Disconnect request to Fortigate.
566500	Activation Failed. FTM Server: provision code not exist (40).
567157	Trusted CA import shows as pending when certificate is using SHA512 as hash.
567493	EAP-TLS authentication does not check AuthorityKeyIdentifier when matching allowed/trusted CAs.
568479	EAP-TLS - deletion of local CA#1 breaks authentication for local CA#2 with identical subject.
569420	Certificate upload to FortiAuthenticator in PKCS#12 format fails.
570138	When accessing Local Users menu under Authentication > User management , error messages are showing intermittently.
571537	Smart Connect profile is not working with MAC computer.
573278	Fortinet SSO Methods > SSO > Portal Services page click to hide elements.
574824	No more than 20 realms can be present in RADIUS client settings.
575996	FortiAuthenticator as RSSO > FSSO processing fails if fails RADIUS Accounting Sources is configured with FQDN instead of IP.
576691	Default realm allowing RADIUS users to authenticate using non-existing realms.
577590	FortiGuard server failed sending SMS because message is too long.
581951	FortiToken Cloud status service error when no entitlement purchased.
581967	FTM trial license activation: Disable "Cannot find req_trial_ftm task. It might have been removed."
582845	Revoked local service certificates not in CRL.
582850	RADIUS attributes are not added in Access-Accept packet.
583729	Unable to import users into LDAP Directory Tree.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.



The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model				
		200E	400E	1000D	2000E	3000E
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20
	User Uploaded Images	39	114	514	1014	2014
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333
	Users (Local + Remote) ¹	500	2000	10000	20000	40000
	User RADIUS Attributes	1500	6000	30000	60000	120000
	User Groups	50	200	1000	2000	4000
	Group RADIUS Attributes	150	150	600	6000	12000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses ²	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	2500	10000	50000	100000	200000
	RADIUS Client Profiles	500	2000	10000	20000	40000

Feature		Model				
		200E	400E	1000D	2000E	3000E
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Users Sync Rule	50	200	1000	2000	4000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
FSSO & Dynamic Policies						
FSSO	FSSO Users	500	2000	10000	20000	200000 ³
	FSSO Groups	250	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	400
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000
Accounting Proxy	Sources	500	2000	10000	20000	40000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100000	200000
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	50000	100000	200000

¹ Users includes both local and remote users.

² **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

³ For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.



The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of auth clients (NAS devices) that can authenticate to the system is:

$$100 / 10 = 10$$

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "-". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
User Management	Users (Local + Remote) ¹	5	*****	100	5000

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) ²	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	RADIUS Client Profiles	3	Users	100	5000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users / 100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

¹ Users includes both local and remote users.

² **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.